Ohio Administrative Code

Rule 5180:1-7-01 Employee access to confidential personal information.

Effective: December 15, 2025

(A) Definitions.

For the purposes of this rule the following definitions apply:

(1) "Access" as a noun means an instance of copying, viewing, or otherwise perceiving whereas "access" as a verb means to copy, view, or otherwise perceive.

(2) "Acquisition of a new computer system" means the purchase of a "computer system," as defined in this rule, that is not a computer system currently in place nor one for which the acquisition process has been initiated as of the effective date of the agency rule promulgated under section 1347.15 of the Revised Code.

(3) "Computer system" means a "system," as defined by section 1347.01 of the Revised Code, that stores, maintains, or retrieves personal information using electronic data processing equipment.

(4) "Confidential personal information" (CPI) has the meaning as defined by division (A)(1) of section 1347.15 of the Revised Code and identified by rules promulgated by the agency in accordance with division (B)(3) of section 1347.15 of the Revised Code that reference the federal or state statutes or administrative rules that make personal information maintained by the agency confidential.

(5) "Employee of the department" means each employee of the Ohio department of children and youth regardless of whether he or she holds an elected or appointed office or position within the agency.

(6) "Incidental contact" means contact with the information that is secondary or tangential to the primary purpose of the activity that resulted in the contact.

(7) "Individual" means a natural person and in the context used in division (C)(1)(b) of section 1347.15 of the Revised Code, and paragraph (E)(4)(b)(iv) of this rule, means the subject of the confidential personal information, or the authorized representative, legal counsel, legal custodian or legal guardian of the subject of the confidential personal information, or any other similarly situated person who is permitted under state or federal law to act on behalf of, or in furtherance of, the interests of the subject of the confidential personal information, such as an executor or administrator appointed by the court or individual granted power of attorney by the subject of the information. "Individual" does not include an opposing party in litigation, or the opposing party's legal counsel, or an investigator, auditor or any other party who is not acting on behalf of, or in furtherance of the interests of, the subject of the confidential personal information, even if such individual has obtained a signed release from the subject of the confidential personal information.

(8) "Information owner" means the individual appointed in accordance with division (A) of section 1347.05 of the Revised Code to be directly responsible for a system.

(9) "Person" means a natural person.

(10) "Personal information" has the same meaning as defined in division (E) of section 1347.01 of the Revised Code.

(11) "Personal information system" means a "system" that "maintains" "personal information" as those terms are defined in section 1347.01 of the Revised Code. "System" includes both records that are manually stored and records that are stored using electronic data processing equipment.

(12) "Research" means a methodical investigation into a subject.

(13) "Routine" means commonplace, regular, habitual, or ordinary.

(14) "System" has the same meaning as defined by division (F) of section 1347.01 of the Revised Code.

(15) "Upgrade" means a substantial redesign of an existing computer system for the purpose of providing a substantial amount of new application functionality, or application modifications that

would involve substantial administrative or fiscal resources to implement, but would not include maintenance, minor updates and patches, or modifications that entail a limited addition of functionality due to changes in business or law.

(16) "The department" means the Ohio department of children and youth.

(B) Procedures for accessing confidential personal information.

(1) Criteria for accessing confidential personal information.

Personal information systems of the department are managed on a "need-to-know" basis whereby the information owner determines the level of access needed for an employee of the department to fulfill his or her job duties. The determination of access to confidential personal information will first be approved by the employee's supervisor and the information owner prior to providing the employee with access to confidential personal information within a personal information system. The department will establish procedures for determining a revision to an employee's access to confidential personal information upon a change to that employee's job duties including, but not limited to, transfer or termination. Whenever an employee's job duties no longer indicate the need for access to confidential personal information in a personal information system, the employee's access to confidential personal information will be removed.

(2) Individual's request for a list of confidential personal information.

Upon the signed written request of any individual for a list of confidential personal information about the individual maintained by the department, the department will do all of the following:

(a) Verify the identity of the individual by a method that provides safeguards commensurate with the risk associated with any unauthorized access to, or use or release of, the confidential personal information;

(b) Provide to the individual the confidential personal information that does not relate to an investigation about the individual or is otherwise not excluded from the scope of Chapter 1347. of the Revised Code; and

(c) If all information relates to an investigation about that individual, determine what, if any, information can be disclosed to the individual who was or is being investigated, provide the individual with any information which is not protected from disclosure, and inform the individual, to the extent that it is legally permitted, of the legal basis for any records that are withheld or redacted.

(3) Notice of invalid access.

(a) Upon discovery or notification that confidential personal information of a person has been accessed by an employee for an invalid reason, the department will notify the person whose information was invalidly accessed as soon as practical, and provide him or her with details of the unauthorized access, to the extent known at the time. However, the department will delay notification for a period of time necessary to ensure that the notification would not delay or impede an investigation or jeopardize homeland or national security. Additionally, the department may delay the notification consistent with any measures necessary to determine the scope of the invalid access, including which individuals' confidential personal information invalidly was accessed, and to restore the reasonable integrity of the system. "Investigation" as used in this paragraph means the investigation of the circumstances and involvement of an employee surrounding the invalid access of the confidential personal information. Once the department determines that notification would not delay or impede an investigation, the department will disclose the access to confidential personal information made for an invalid reason to the person.

(b) Notification provided by the department will inform the person of the type of confidential personal information accessed and the date or dates of the invalid access, if known.

(c) Notification may be made by any method reasonably designed to accurately inform the person of the invalid access, including written, electronic, or telephone notice.

(4) Appointment of a data privacy point of contact and completion of a privacy impact assessment.

(a) The department's director will designate an employee of the department to serve as the data privacy point of contact under the working title of "DCY chief privacy officer."

(b) The DCY chief privacy officer will work with the state of Ohio chief privacy officer and the state of Ohio chief information security officer within the state of Ohio office of information technology to assist the department with both the implementation of privacy protections for the confidential personal information that the department maintains and compliance with section 1347.15 of the Revised Code and the rules adopted thereunder.

(c) The DCY chief privacy officer will ensure the timely completion of the "privacy impact assessment form" developed by the state of Ohio office of information technology.

(C) Valid reasons for accessing confidential personal information.

Pursuant to division (B)(2) of section 1347.15 of the Revised Code, this rule contains a list of valid reasons, directly related to the department's exercise of its powers or duties, for which only employees of the department may access confidential personal information regardless of whether the personal information system is manual or electronic.

(1) Except as prohibited by federal or state law, performing the following functions constitute valid reasons for authorized employees of the department to access confidential personal information:

(a) Responding to a request from an individual for the list of confidential personal information or records the department maintains on that individual;

(b) Responding to a public records request;

(c) Administering a constitutional provision or duty;

(d) Administering a statutory provision or duty connected to the department or its programs;

(e) Administering an administrative rule provision or duty connected to the department or its programs;

(f) Complying with any state or federal program requirements;

(g) Processing or payment of claims or otherwise administering a program with individual participants or beneficiaries;

(h) Auditing or monitoring purposes;

(i) Licensure (or permit, eligibility, filing, etc.) processes;

(j) Investigation or law enforcement purposes, when permitted by any applicable programmatic laws or regulations;

(k) Administrative hearings;

(l) Litigation, complying with an order of the court, or subpoena;

(m) Human resource matters (e.g., hiring, promotion, demotion, discharge, salary/compensation issues, leave requests/issues, timecard approvals/issues);

(n) Complying with an executive order or policy;

(o) Complying with a department policy or a state administrative policy issued by the department of administrative services, the office of budget and management or other similar state agency;

(p) Complying with a collective bargaining agreement provision; or

(q) Research in the furtherance of department-specific programs in so far as allowed by statute.

(2) To the extent that the general processes described in paragraph (C)(1) of this rule do not cover the circumstances under consideration, for the purpose of carrying out specific duties of the department, authorized employees would also have valid reasons for accessing confidential personal information as set forth in any applicable policy or rule adopted by the department.

(D) Confidentiality Statutes.

The federal statutes and regulations and state statutes and administrative rules listed in the appendix to this rule make personal information maintained by the agency confidential and identify the confidential personal information that are subject to rules promulgated by this agency in accordance with section 1347.15 of the Revised Code.

(E) Restricting and logging access to confidential personal information systems.

For personal information systems that are computer systems and contain confidential personal information, the department will do the following:

(1) Access restrictions.

Access to confidential personal information that is kept electronically will warrant a password or other sufficient authentication measure as determined by the DCY chief privacy officer.

(2) Acquisition of a new computer system.

When the department acquires a new computer system that stores, manages or contains confidential personal information, the department will include a mechanism for recording specific access by employees of the department to confidential personal information in the system.

(3) Upgrading existing computer systems.

When the department modifies an existing computer system that stores, manages or contains confidential personal information, that results in over half of the lines of code associated with that system being modified, then that system will have an automated mechanism for recording specific access by employees of the department to any confidential personal information that is accessed via that system.

(4) Logging confidential personal information in existing computer systems.

(a) The department will ensure that employees of the department who access confidential personal information within the department's computer systems maintain a log that records that access.

(b) Access to confidential information is not to be entered into the log under the following circumstances:

(i) The employee of the department is accessing confidential personal information for official agency purposes, including research, and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(ii) The employee of the department is accessing confidential personal information for routine office procedures and the access is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iii) The employee of the department comes into incidental contact with confidential personal information and the access of the information is not specifically directed toward a specifically named individual or a group of specifically named individuals.

(iv) The employee of the department accesses confidential personal information about an individual based upon a request made under either of the following circumstances:

(a) The individual requests confidential personal information about himself or herself.

(b) The individual makes a request that the department takes some action on that individual's behalf and the confidential personal information is accessed in order to consider or process that request.

(c) The department will use a consistent electronic means for logging where reasonably possible. If the logging process is already being achieved through existing means, then no additional logging is needed in those instances.

(5) Nothing in this rule limits the agency from requiring logging in any circumstance that it deems necessary.